E-ISSN: 2717-4581 | P-ISSN: 2783-1345

Innovation Management and Operational Strategies

www.journal-imos.ir

Inov. Manage. Oper. Stra. Vol. 3, No. 3 (2022) 356–370.

Paper Type: Original Article

Identification and Ranking of Security Indicators in Online Social Networks Using MADM Technique

Alireza Amini [1,*], Hamed Fathi[1]

[1] *Department of Industrial Engineering, Ayandegan Institute of Higher Education, Tonekabon, Iran; alirezaamini@iran.ir.*

Citation:

Amini, A., & Fathi, H. (2022). Identification and ranking of security indicators in online social networks using MADM technique. *Innovation management and operational strategies, 3(3),* 356-370.

Received: 05/02/2022 Reviewed: 13/03/2022 Revised: 23/05/2022 Accepted: 24/05/2022

Abstract

Purpose: This study aims to identify and rank security indicators in online social networks. Social networks include Facebook, Twitter, Telegram, WhatsApp, YouTube, and Instagram.

Methodology: The information technology units of Melli Bank have been studied, and 30 people have been considered research experts. For this purpose, seven important indicators were identified, and the TOPSIS technique was used to prioritize them. Then, the relationship between the identified indicators and online social network security was investigated using the Spearman correlation test. For this purpose, a questionnaire with 24 items was distributed, and 262 samples were collected and analyzed.

Findings: The results show that security indicators in online social networks in order of priority are implementing authentication and licensing mechanisms, using up-to-date software and avoiding suspicious programs, restricting personal information dissemination, monitoring to prevent unauthorized processing of information, compliance with standards the country's IT infrastructure, and the installing an intruder detection system. Also, based on the results of the Spearman correlation test, all factors have had a positive and significant effect on social network security.

Originality/Value: In this study, we concluded that there is a significant relationship between the influential factors and the security of social networks on the line defined for these networks. The development of information and communication technology infrastructures and the increase in users using virtual social networks justifies the need to create and develop a mechanism for establishing security in these communication networks.

Keywords: Iran IT infrastructure, Dissemination of personal information, Security, Online social networks, TOPSIS.

Corresponding Author: alirezaamini@iran.ir

http://dorl.net/dor/20.1001.1.27831345.1401.3.3.7.4

Innovation Management & Operational Strategies

مدیریت نوآوری و راهبردهای عملیاتی

دوره ۳، شماره (۳)، (۱۴۰۱)، ۳۷۰-۳۵۶

www.journal-imos.ir



نوع مقاله: پژوهشی

شناسایی و رتبه‌بندی شاخص‌های امنیتی در شبکه‌های اجتماعی برخط با تکنیک MADM

علیرضا امینی[1*]، حامدفتحی[1]

[1] گروه مهندسی صنایع، موسسه آموزش عالی آیندگان، تنکابن، ایران.

چکیده

هدف: هدف از تحقیق حاضر شناسایی و رتبه‌بندی شاخص‌های امنیتی در شبکه‌های اجتماعی بر خط می‌باشد. شبکه‌های اجتماعی مانند فیس‌بوک، توییتر، تلگرام، واتساپ، یوتیوب و اینستاگرام می‌باشند.

روش‌شناسی پژوهش: واحدهای فناوری اطلاعات بانک ملی موردمطالعه قرار گرفته که تعداد ۳۰ نفر به به‌عنوان خبرگان پژوهش در نظر گرفته شده است. بدین منظور، هفت شاخص مهم شناسایی گردید و به‌منظور اولویت‌بندی شاخص‌ها از تکنیک *TOPSIS* استفاده گردید. در این مرحله نیز پرسشنامه مقایسات زوجی برای خبرگان پژوهش توزیع و گردآوری گردید و بر اساس آن اولویت‌بندی عوامل ارائه شده است. درنهایت با استفاده از آزمون همبستگی اسپیرمن به بررسی ارتباط بین شاخص‌های شناسایی‌شده و امنیت در شبکه‌های اجتماعی بر خط پرداخته شد. بدین منظور نیز پرسشنامه‌ای با ٢٤ گویه توزیع و تعداد ٢٦٢ نمونه جمع‌آوری و مورد تحلیل قرار گرفت.

یافته‌ها: نتیجه تحقیق نشان می‌دهد شاخص‌های امنیتی در شبکه‌های اجتماعی بر خط به ترتیب اولویت عبارت‌اند از: پیاده‌سازی سازوکارهای تصدیق هویت و مجوزدهی، استفاده از نرم‌افزارهای به‌روز و پرهیز از برنامه‌های مشکوک، محدودیت انتشار اطلاعات شخصی، پایش به‌منظور عدم‌پردازش غیرمجاز اطلاعات، رعایت استانداردهای امنیتی، زیرساخت‌های *IT* کشور و نصب سیستم شناساگر متجاوز. همچنین بر اساس نتایج آزمون همبستگی اسپیرمن، کلیه عوامل تاثیر مثبت و معناداری بر امنیت شبکه‌های اجتماعی داشته‌اند.

اصالت/ارزش افزوده علمی: ما در این تحقیق به این نتیجه رسیدیم که بین عوامل موثر و امنیت شبکه‌های اجتماعی بر خط تعریف‌شده برای این شبکه‌ها، رابطه معناداری دارد. در واقع توسعه‌ی زیرساخت‌های فناوری اطلاعات و ارتباطات و افزایش شمار کاربران استفاده‌کننده از شبکه‌های اجتماعی مجازی، لزوم ایجاد و توسعه‌ی سازوکاری برای برقراری امنیت در این شبکه‌های ارتباطی را توجیه می‌کند.

کلیدواژه‌ها: زیرساخت‌های *IT* ایران، انتشار اطلاعات شخصی، امنیت، شبکه‌های اجتماعی بر خط، تاپسیس.

۱- مقدمه

اخیرا، رایج‌ترین فناوری که تقریبا همه افراد از آن استفاده روزانه می‌کنند، اینترنت است. با استفاده از فناوری اینترنت، هر فرد در هر جای جهان حتی با تجربه بسیار محدود از فناوری اطلاعات، می‌تواند ارتباط برقرار کند، اطلاعات را به اشتراک بگذارد، بازی کند و بسیاری از

* نویسنده مسئول

alirezaamini@iran.ir

http://dorl.net/dor/20.1001.1.27831345.1401.3.3.7.4

موارد دیگر از اینترنت را به روشی آسان و تقریبا رایگان تجربه کند (زباری و همکاران[1]، ۲۰۲۰). یکی از این کاربردها که تقریبا همه به‌طور روزانه استفاده می‌کنند، رسانه‌های اجتماعی هستند.

رسانه‌های اجتماعی مجموعه‌ای از وب‌سایت‌های مبتنی بر اینترنت است. هدف و عملکرد رسانه‌های اجتماعی ترویج تعامل شخصی و متمرکز بر مشاغل افراد در سراسر جهان است (ادوسوموان و همکاران[2]، ۲۰۱۱). رسانه‌های اجتماعی سرویسی است که به کاربران امکان می‌دهد مطالب را به اشتراک بگذارند. مطالب انواع مختلفی از اطلاعات (پیام‌ها، اسناد، فیلم‌ها) در موضوعات مختلف هستند. علاوه بر این، این سرویس همچنین به کاربران امکان می‌دهد ایده‌ها، نظرات و افکار جدیدی را با بسیاری از افراد به اشتراک بگذارند (مک کارول و کران[3]، ۲۰۱۳).

در دهه گذشته، شبکه‌های اجتماعی، مانند فیس‌بوک، توییتر، تلگرام، واتساپ، یوتیوب و اینستاگرام رشد سریعی در تعداد کاربران داشته‌اند (اورتیس-اوسپینا[4]، ۲۰۱۹). دلیل آن این است که این ابزار به‌طور گسترده‌ای مورداستفاده قرار گرفته است، به‌ویژه با گسترش استفاده از تلفن‌های هوشمند به‌عنوان راهی برای برقراری ارتباط، به اشتراک‌گذاری دانش، به اشتراک‌گذاری افکار، عکس‌ها و فیلم‌ها و بسیاری از ویژگی‌های دیگر که افراد بیشتری را در سراسر جهان جذب می‌کند. سایت‌های شبکه‌های اجتماعی می‌توانند ابزارهای فروش و بازاریابی ارزشمندی باشند و همچنین انحرافات سرگرم کننده‌ای باشند (چفی[5]، ۲۰۲۲).

از طرفی، در عصر فرامدرن امروز، امنیت از تحولات وسیع‌تر در سیستم جهانی، گسترش ارتباطات، پیشرفت‌های فناوری و ارتباطات نزدیک‌تر جوامع با یکدیگر، متاثر گردیده است (رسولی و بندگی منفرد[6]، ۲۰۱۴). امروزه، توسعه فناوری ارتباطات و در پی آن گسترش شبکه‌های اجتماعی، به کلیدی‌ترین ابزار تهدیدات نرم علیه افراد و جوامع هدف تبدیل شده است (محکم‌کار و حلاج[7]، ۲۰۱۴). شبکه‌های اجتماعی، نسل جدیدی از پایگاه‌هایی هستند که این روزها در کانون توجه کاربران شبکه‌های جهانی اینترنت قرار گرفته‌اند در حال حاضر می‌توان از شبکه‌های اجتماعی به‌عنوان یکی از برجسته‌ترین دستاوردهای انقلاب اطلاعاتی نام برد، با معنایی تازه بخشیدن به ارتباطات باعث تغییرات بنیادی در تعاملات افراد گردیده است. با پیدایش شبکه‌های اجتماعی، امکاناتی همچون برقراری ارتباط نوشتاری، گفتاری و دیداری با هزینه نسبتاً کم در زمان کم فراهم گردیده است. از سوی دیگر، فراگیر شدن شبکه‌های اجتماعی خود منشا تهدیدات زیادی گردیده‌اند (عبدالرحمانی و همکاران[8]، ۲۰۱۸).

در این میان حجم زیادی از داده‌ها که نشان‌دهنده علایق، دیدگاه‌ها و نظرات افراد است در بستر شبکه‌های اجتماعی مانند فیس بوک، توییتر تا پیام‌رسان‌هایی مانند واتساپ، تلگرام، اینستاگرام به اشتراک گذاشته می‌شود. اکثر شبکه‌های اجتماعی از شماره موبایل یا آدرس ایمیل برای ثبت‌نام کاربران استفاده می‌کنند. پروفایل شخصی افراد در این شبکه‌ها به همراه مطالبی که توسط کاربر در این شبکه‌ها منتشر می‌شود و پاسخ‌هایی که از سوی کاربر در پاسخ به یک مطلب گذاشته می‌شود می‌تواند مورد تحلیل قرار گیرد تا جایی که ویژگی‌های شخصیتی افراد را می‌توان از طریق مطالبی که موردپسند او قرار گرفته است تا حد بسیار دقیقی مشخص کرد. این قابلیت‌هایی که در نتیجه تحلیل داده‌های شبکه اجتماعی وجود دارد به‌طور بالقوه حریم خصوصی را در خطر قرار می‌دهد به نحوی که در آخرین رسوایی در این زمینه، شرکت کمبریج آنالتیکا توانست به اطلاعات ۵۰ میلیون نفر از کاربران فیسبوک دست یابند و از این اطلاعات در جهت هدایت کمپین‌های انتخاباتی آمریکا و تاثیرگذاری بر روی آن استفاده کند (بولمنستوک و همکاران[9]، ۲۰۱۹).

بنابراین، توجه به بحث شناسایی ابزارها، اصول و راهکارهای ارتقاء امنیت داده و همچنین حفظ حریم خصوصی یکی از ضرورت‌های اساسی در شبکه‌های اجتماعی است. از این رو به موازات رشد بی‌سابقه استفاده از شبکه‌های اجتماعی در کشور ایران و تلاش‌های مسئولان دولتی از جمله وزارتخانه‌های ارتباطات و فناوری اطلاعات و فرهنگ و ارشاد اسلامی برای آموزش سواد رسانه‌ای در بین کاربران شبکه‌های اجتماعی، نزدیک به دو سال است که کاربران با آسیب‌های مختلفی از جمله سوءاستفاده از اطلاعات شخصی خود روبه‌رو

---

[1] Zeebaree et al.
[2] Edosomwan et al.
[3] McCarroll and Curran
[4] Ortiz-Ospina
[5] Chaffey
[6] Rasooli and Bandegi Monfared
[7] Mohkamkar and Halaj
[8] Abdulrahmani e al.
[9] Blumenstock et al.

شده‌اند. بر اساس آمارهای به‌دست‌آمده از سازمان امور فضایی، اکثر مراجعات امروزی شهروندان به سازمان‌های حقوقی در راستای مبحث سو استفاده‌های انجام‌شده از حریم شخصی آن‌ها در شبکه‌های اجتماعی است بر همین اساس وزارت ارتباطات و فناوری اطلاعات با همکاری سایر نهادهای مربوطه زیرساخت طرح‌های مختلفی را درباره مبارزه با آسیب‌های امنیتی شبکه‌های اجتماعی در دستور کار قرار داد که بسیاری از آن‌ها در حال حاضر در مرحله اجرا قرار دارد؛ بنابراین، این سوال مطرح می‌گردد که چه عوامل امنیتی در ارتباط با شبکه‌های اجتماعی حائز اهمیت هستند و کدام‌یک در اولویت بیشتری قرار دارند؟ در همین راستا، هدف این پژوهش شناسایی و رتبه‌بندی شاخص‌های امنیتی در شبکه‌های اجتماعی بر خط می‌باشد.

۲- مبانی نظری پژوهش

۲-۱- امنیت شبکه‌های اجتماعی برخط

با پیشرفت تمدن و شکل‌گیری جوامع، محدوده امنیت، ابعاد بسیار گسترده‌تری یافت و با تفکیک حوزه اموال و حقوق شخصی افراد از یکدیگر و از اموال عمومی و همچنین تعریف قلمروهای ملی و بین‌المللی، به تدریج مفاهیم وسیعی مانند حریم خصوصی، امنیت اجتماعی، امنیت مالی امنیت سیاسی، امنیت ملی و امنیت اقتصادی را نیز شامل گردید. این مفاهیم گرچه دیگر کاملا محدود به نیازهای فیزیکی بشر نمی‌شدند، ولی عمدتا تحقق و دستیابی به آن‌ها مستلزم وجود و یا استفاده از محیط‌های واقعی و فیزیکی بود. لیکن جهان در دهه‌های اخیر و به‌ویژه در پنج سال گذشته عرصه تحولات چشمگیری بوده که بسیاری از مناسبات و معادلات پیشین را به‌طور اساسی دستخوش تغییر نموده است. این تحولات که با محوریت کاربری وسیع از فناوری اطلاعات و ارتباطات امکان‌پذیر شده، از کاربرد رایانه به‌عنوان ابزار خودکارسازی و افزایش بهره‌وری آغاز گردیده و اکنون با تکامل کاربری آن در ایجاد فضای هم‌افزایی مشارکتی، عملا زندگی فردی و اجتماعی بشر را دگرگون ساخته است. به باور بسیاری از صاحب‌نظران همان‌گونه که پیدایش خط و کتابت آن‌چنان تاثیر شگرفی بر سرنوشت انسان بر جای گذاشته ورود به فضای مجازی حاصل از فناوری نوین اطلاعات و ارتباطات نیز دوره جدیدی از تمدن بشری را رقم زده، به نحوی که انقلاب عصر اطلاعات شیوه اندیشه، تولید، مصرف، تجارت، مدیریت، ارتباط، جنگ را دگرگون ساخته است. اینترنت به‌عنوان یکی از مهم‌ترین ابداعات بشر در قرن اخیر، با قابلیت‌ها و کارکردهای متعدد و گسترده‌اش، بخش‌های مختلف زندگی انسان را تحت تاثیرات مثبت و منفی خود قرار داده است. مبنا و هدف اصلی اینترنت، برداشتن فاصله جغرافیایی میان آنان سراسر دنیا و ایجاد تحول در عرصه ارتباطات و تبادل اطلاعات است. درحالی‌که هنوز هیچ‌کس تصور نمی‌کرد که روزی جنبه اجتماعی اینترنت به‌صورت کاربرد اصلی آن در آید، شبکه‌های اجتماعی اینترنتی پای به عرصه وجود گذاشتند که ظهور آن‌ها یکی از مهم‌ترین رویدادها و دستاوردهای مهم فناوری اطلاعات و ارتباطات در دهه‌های اخیر بوده است (بولمنستوک و همکاران، ۲۰۱۹).

شبکه‌های اجتماعی، نسل جدیدی از پایگاه‌هایی هستند که این روزها در کانون توجه کاربران شبکه‌های جهانی اینترنت قرار گرفته‌اند. این‌گونه پایگاه‌ها بر مبنای تشکیلات آنلاین فعالیت می‌کنند و هرکدام دسته‌ای از کاربران اینترنتی با ویژگی خاص را گرد هم می‌آورند. شبکه‌های اجتماعی را گونه‌ای از رسانه‌های اجتماعی می‌دانند که امکان دستیابی به شکل جدیدی از برقراری ارتباط و به اشتراک‌گذاری محتوا در اینترنت را فراهم آورده‌اند. در واقع شبکه‌های اجتماعی پدیده فراگیر عصر حاضر هستند که فرآیند تعامل افراد با یکدیگر را تسهیل می‌کنند. در این میان حجم زیادی از داده‌ها که نشان‌دهنده علایق، دیدگاه‌ها و نظرات افراد است در بستر شبکه‌های اجتماعی مانند فیس‌بوک، توییتر تا پیام‌رسان‌هایی مانند واتساپ، تلگرام، اینستاگرام به اشتراک گذاشته می‌شود. اکثر شبکه‌های اجتماعی از شماره موبایل یا آدرس ایمیل برای ثبت‌نام کاربران استفاده می‌کنند. پروفایل شخصی افراد در این شبکه‌ها به همراه مطالبی که توسط کاربر در این شبکه‌ها منتشر می‌شود و پاسخ‌هایی که از سوی کاربر در پاسخ به یک مطلب گذاشته می‌شود می‌تواند مورد تحلیل قرار گیرد تا جایی که ویژگی‌های شخصیتی افراد را می‌توان از طریق مطالبی که موردپسند او قرار گرفته است تا حد بسیار دقیقی مشخص کرد. این قابلیت‌هایی که در نتیجه تحلیل داده‌های شبکه اجتماعی وجود دارد به‌طور بالقوه حریم خصوصی را در خطر قرار می‌دهد به‌نحوی‌که در آخرین رسوایی در این زمینه، شرکت کمبریج آنالتیکا توانست به اطلاعات ۵۰ میلیون نفر از کاربران فیس‌بوک دست یابند و از این اطلاعات در جهت هدایت کمپین‌های انتخاباتی آمریکا و تاثیرگذاری بر روی آن استفاده کند (بولمنستوک و همکاران، ۲۰۱۹).

۳- پیشینه پژوهش

۳-۱- مطالعات داخلی

زارع زاده[1] (۲۰۲۱)، به بررسی آسیب‌ها و چالش‌های امنیتی سازی مسائل داخلی؛ مطالعه موردی شبکه‌های اجتماعی مجازی، فصلنامه مطالعات راهبردی پرداختند و روش پژوهش کتابخانه‌ای - اسنادی بود. نویسنده ضمن اذعان به سخت‌تر بودن امنیتی سازی مسائل داخلی نسبت به مسائل خارجی، معتقد است که مواردی نظیر تعدد بازیگران تصمیم گیر و ابهام در صلاحیت بازیگر امنیتی ساز، چارچوب‌بندی و تصویرسازی نامناسب از تهدید، بی‌توجهی یا کم‌توجهی به ویژگی‌های بافت اجتماعی و تنوع مخاطبان، سیاست‌گذاری نامناسب و غیرامنیتی نکردن به‌موقع از مهم‌ترین عواملی بوده که امنیتی سازی شبکه‌های اجتماعی مجازی را در جمهوری اسلامی ایران با چالش مواجه کرده است. محمدرضایی[2] (۲۰۲۱)، به بررسی تشخیص کاربران جعلی در شبکه‌های اجتماعی با استفاده از تحلیل مولفه‌های اصلی و الگوریتم تخمین چگالی هسته پرداختند و در روش پیشنهادی برای آموزش ماشین از ویژگی‌های شباهت مختلفی مانند شباهت کسینوس، شباهت جاکارد، شباهت شبکه دوستی و معیارهای مرکزیت استفاده می‌شود که همه این ویژگی‌ها از ماتریس مجاورت گراف شبکه اجتماعی استخراج می‌شوند. در ادامه جهت کاهش ابعاد داده‌ها و حل مشکل بیش برازش از تحلیل مولفه‌های اصلی استفاده شد. سپس با استفاده از دسته‌بندهای تخمین چگالی هسته و الگوریتم شبکه عصبی خودسازمان‌ده داده‌ها دسته‌بندی‌شده و نتایج روش پیشنهادی با استفاده از معیارهای دقت، حساسیت و نرخ تشخیص اشتباه ارزیابی می‌شود. بررسی نتایج نشان می‌دهد، روش پیشنهادی با دقت ۹۹/۶% کاربران جعلی را تشخیص می‌دهد که نسبت به روش کاوو حدود ۵% بهبود یافته است، همچنین نرخ تشخیص اشتباه کاربران جعلی نیز نسبت به همین روش ۳% بهبود پیدا کرد. دعاگویان و خیراندیش[3] (۲۰۲۱)، به بررسی تاثیر شبکه‌های اجتماعی تحت تلفن همراه در روابط اجتماعی خانواده‌های مناطق غربی تهران بزرگ پرداختند و شبکه اجتماعی تلگرام را موردمطالعه قرار دادند. در این پژوهش در مورد تاثیر محتوای صوتی- تصویری و چندرسانه‌ای تلگرام بر روابط اجتماعی خانواده‌ها، تاثیر اشاعه فرهنگ هنجارشکنی اخلاقی در تلگرام بر روابط اجتماعی خانواده‌ها، تاثیر اعتیاد مجازی در تلگرام بر روابط اجتماعی خانواده‌ها، تاثیر ایجاد هویت کاذب در تلگرام بر روابط اجتماعی خانواده‌ها، تاثیر اشاعه فرهنگ مدگرایی در تلگرام بر روابط اجتماعی خانواده‌ها و تاثیر اشاعه فرقه‌های نوظهور در تلگرام بر روابط اجتماعی خانواده‌ها مطرح گردید. نتایج نشان داد شبکه اجتماعی تلگرام بیشترین تاثیر را بر ایجاد هویت کاذب و کمترین تاثیر را بر اشاعه فرقه‌های نوظهور دارد. ندری و همکاران[4] (۲۰۱۹)، پژوهشی در موردبررسی نقش سیاسی- امنیتی شبکه‌های اجتماعی مجازی بر امنیت ملی جمهوری اسلامی ایران انجام دادند و روش پژوهش حاضر روش تحلیل محتوای کیفی و جامعه آماری آن را صاحب‌نظران و نخبگان حوزه امنیت و فضای مجازی تشکیل داده‌اند. حجم نمونه در گروه مذکور بر اساس اشباع مقوله‌ها و اطلاعات شناسایی‌شده ۱۳ نفر بود. یافته‌های پژوهش نشان می‌دهد شبکه‌های اجتماعی مجازی مانند شمشیر دو لبه‌ای هستند که می‌توانند مجموعه‌ای از کنش‌های مثبت و منفی را در محیط سیاسی- امنیتی جمهوری اسلامی ایجاد نمایند. در وضعیت فعلی به علت رهاشدگی و سیاست‌گذاری جزیره‌ای فضای مجازی در جمهوری اسلامی ایران، شبکه‌های اجتماعی آسیب‌پذیری کشور را در برخی مؤلفه‌های امنیت ملی برجسته کرده است. این شبکه‌ها هم‌اکنون به‌طورجدی در جهت تخریب و القای ناکارآمدی نظام جمهوری اسلامی ایران هنجارسازی معارض، مشروعیت زدایی ساختاری از نظام سیاسی، تضعیف انسجام ملی و شکاف بین جامعه و حاکمیت و ایجاد زمینه تقابل مردم با نظام سیاسی و تضعیف باورهای ملی فعالیت می‌کنند و در حوزه امنیتی نیز با کارکرد جاسوسی و پایش اطلاعات کاربران، مهیاسازی ابزار ارتباطی گروه‌های برانداز، جمع‌آوری اطلاعات افراد و مشاغل خاص، آموزش‌های مخرب در بستر شبکه‌های اجتماعی و انتقال اطلاعات طبقه‌بندی در جهت مخدوش سازی امنیت ملی فعالیت می‌کنند. تاسیس ساختاری قدرتمند و فرا قوه‌ای برای سیاست‌گذاری و ساماندهی فضای مجازی کشور و راه‌اندازی شبکه ملی اطلاعات می‌تواند در رفع بسیاری از مشکلات در این حوزه موثر باشد.

محمدی و همکاران[5] (۲۰۱۹)، در تحقیقی فیلترینگ شبکه‌های اجتماعی و نقش آن در حفظ و امنیت حقوق شهروندی در پدافند سایبری در ایران را موردبررسی قرار داده‌اند. نقش منفی فیلترینگ شبه‌های اجتماعی در حفظ امنیت و حقوق شهروندی عبارت‌اند از: کاهش در

---

[1] zarezadeh
[2] Mohamadrezae
[3] Doaguyan and Kheirandish
[4] Nadri et al.
[5] Mohamadi et al.

آمد افرادو نقض حق کار افراد عدم دسترسی به اطلاعات به‌روز و کار آمد و نقض حق دسترسی به اخبار و اطلاعات، عدم برقراری ارتباط با افراد دیگر و نقض حق تعامل نقش مثبت فیلترینگ شبه‌های اجتماعی در حفظ امنیت و حقوق شهروندی بارند از: امنیت روانی به دنبال عدم پخش تصاویر و موضوعات نابهنجار، افزایش کسب‌وکار داخلی و عدم تبلیغ کالاهای بیگانه در نتیجه توسعه کار، انسجام خانواده‌ها و جلوگیری از بی‌بندوباری‌ها، عدم نقض حریم خصوصی افراد. رسولی و جعفری[1] (۲۰۲۰)، در تحقیقی به بررسی و مقایسه نحوه عملکرد الگوریتم‌های رمزنگاری در امنیت شبکه پرداخته‌اند. رمزنگاری، یک تابع ریاضی است که در فرآیند رمزگذاری و رمزگشایی از این الگوریتم ریاضی استفاده می‌شود. با کمک این الگوریتم، داده‌ها و اطلاعات به شکلی رمزگذاری می‌شود که تنها برای افرادی مشخص و مجاز که رمز و الگوریتم رمزگشایی را می‌دانند قابل‌مشاهده است. در طی سالیان این قبیل الگوریتم‌ها در حال تغییر هستند و از نظر امنیتی پیشرفت داشته‌اند. مهرگان و صدقی وش[2] (۲۰۲۰)، در تحقیقی به مطالعه و بررسی راهکارهای امنیت در شبکه‌های اجتماعی پرداخته‌اند. شبکه‌های اجتماعی در کنار مزایای بی‌شمارش، معایبی نیز دارد که عدم آشنایی کامل با فضای مجازی می‌تواند آسیب‌هایی را برای خانواده‌ها به بار آورد. در این شبکه‌ها داده‌ها به‌صورت مکرر به اشتراک گذاشته می‌شوند و با توجه به این امر بحث امنیت در فضای مجازی به‌شدت احساس می‌شود. امنیت اطلاعات به معنای واقعی یعنی با استفاده از یکسری فرآیندها از دسترس غیرمجاز به اطلاعات و یا محصولات و اعمال تغییرات یا حذف کردن آن‌ها جلوگیری کنیم. یکی از مهم‌ترین مسائلی که از چالش‌های امنیتی در این شماره‌ها به کار می‌رود، نگهداری و امنیت اطلاعات و داده‌های به اشتراک گذاشته‌شده توسط کاربران از دسترسی‌های غیرمجاز و افشای ناخواسته است. در این مقاله با بررسی ابعاد مختلف و نقش‌های تاثیرگذار در امنیت شبکه‌های اجتماعی سعی شده است که راه‌حل‌هایی مطمئن برای بالا بردن امنیت در این شبکه‌ها ارائه گردد. صحافی زاده و ترک لادانی[3] (۲۰۲۰)، در تحقیقی کنترل شایعه در شبکه‌های اجتماعی با استفاده از سازوکارهای امنیت نرم را موردبررسی قرار داده‌اند. در سال‌های اخیر، رواج شایعت در شبکه‌های اجتماعی که به‌ویژه با هدف فریب افکار عمومی ساخته می‌شوند، به یکی از نگرانی‌های جدید در جوامع مختلف تبدیل شده است. شایعات می‌تواند با قصد آسیب‌رسانی در حوزه‌های مختلف مدیریتی و انجام عملیات جنگ نرم تهدید و هدایت شود؛ بنابراین، با توجه به حجم بالای شایعات و لزوم کنترل سریع آن‌ها، توسعه مدل‌هایی برای تحلیل نحوه انتشار شایعات و ارزیابی کارایی و اثربخشی سازوکارهای مختلف مقابله با شایعه از اهمیت ویژه‌ای برخوردار است. در این مقاله مدلی برای انتشارش و کنترل شایعه به‌عنوان یک تهدید نرم در شبکه‌های اجتماعی ارائه شده است. این مدل با تکیه بر ساز و کارهای امنیت نرم مانند اعتماد اعتبار منابع و منتشرکنندگان خبر و رتبه دهی به خبر، شایعه را با استفاده از خرد جمعی کنترل می‌کند. مدل پیشنهادی به‌صورت شبیه‌سازی عامل ـ مبنا بر روی دو شبکه باراباسی ـ آلبرت و شبکه‌ای از مجموعه داده‌های واقعی توییتر با استفاده از روش مونت‌کارلو ارزیابی شده است. نتایج ارزیابی نشان می‌دهند که سازوکار پیشنهادی کنترل شایعه می‌تواند روشی کارا برای کنترل شایعه در شبکه‌های اجتماعی باشد و توسعه‌دهندگان این شبکه‌ها می‌توانند با استفاده از روش پیشنهادی و ارائه امکانات لازم بستری برای خودکنترلی شایعه توسط کاربران فراهم نمایند.

احمدی و واعظی[4] (۲۰۱۹) در تحقیقی رویکردی جهت افزایش امنیت و حفظ حریم خصوصی در شبکه‌های اجتماعی را موردبررسی قرار داده‌اند. در ابتدا چالش امنیت و حفظ حریم خصوصی در شبکه‌های اجتماعی را بیان کرده تا راه‌حل‌هایی به‌منظور کاهش تضادهای طراحی به دست آید. سپس سعی در بهبود این چالش‌ها با ارائه‌ی رویکردی جدیدی است. در این رویکرد جدید از فیلتر بلوم به‌عنوان فیلتر و رمزگذار جهت ایجاد امنیت و حفظ حریم خصوصی استفاده شده است. نتایج شبیه‌سازی و مقایسه شبکه شبیه‌سازی‌شده در حالت بدون فیلتر بلوم و با فیلتر و اعمال تست‌های امنیتی بر روی شبکه‌ها حاکی از موثر بودن رویکرد جدید دارد. زارع و نوروزی[5] (۲۰۱۹)، در تحقیقی به ارزیابی امنیت در خصوص شبکه‌های اجتماعی الگوریتم دسته ذرات پرداخته‌اند. با استفاده از شبکه‌های اجتماعی، کاربران می‌توانند از امکاناتی که تا پیش‌ازاین از طریق سایت‌های مختلف دریافت می‌کردند را یکجا با عضویت در یک شبک اجتماعی در اختیار داشته باشند و به همین دلیل کاربران اغلب زمان آنلاین خود را در شبکه‌های اختصاصی اختصاص می‌دهند.

بابائی[6] (۲۰۱۸)، به بررسی تهدیدهای فضای مجازی و شبکه‌های اجتماعی در امنیت داخلی ناجا پرداخت. این مطالعه با طرح دیدگاه‌های مقام معظم رهبری (مدظله‌العالی) و اندیشه‌ها و دیدگاه‌های صاحب‌نظران حوزه فضای مجازی و شبکه‌های اجتماعی، ابتدا با بیان فرصت‌ها

[1] Rasouli and Jafari
[2] Mehregan and Sedqivash
[3] Sahafizadeh and Torkladani
[4] Ahmadi and Vaezi
[5] Zare and Norouzi
[6] Babaei

و تهدیدهای این حوزه در عصر کنونی؛ به دغدغه‌های امنیتی ناشی از عضویت کارکنان ناجا در فضای مجازی و تهدیدها و آسیب‌هایی که کارکنان و در راس امنیت داخلی ناجا را تهدید می‌کند پرداخته و حفاظت اطلاعات ناجا را به‌عنوان یک سازمان تامین‌کننده امنیت داخلی ناجا، ملزم می‌داند که با ارائه راه‌کارهای مناسب و پیشگیرانه و بر پایه روش‌های نوین آموزش و آگاه‌سازی و نه فقط با اعمال محدودیت و خودداری از عضویت کارکنان ناجا در شبکه‌های اجتماعی، به وظیفه صیانتی خود عمل نماید. غیوری ثالث و همکاران[1] (۲۰۱۸)، در تحقیقی به ارائه روشی برای یافتن عامل‌های پرنفوذ در انتشار اطلاعات در شبکه‌های اجتماعی مبتنی بر نظریه آنتروپی پرداختند و ضمن معرفی و محاسبه دو نوع عامل پر اهمیت در انتشار اطلاعات (عامل‌های مرجع و فعال)، روشی برای یافتن این دودسته عامل‌های پراهمیت در انتشار اطلاعات در شبکه‌های اجتماعی برخط مبتنی بر نظریه آنتروپی ارائه و پیاده‌سازی شده است. روش پیشنهادی مبتنی است بر ارزیابی آنتروپی گراف شبکه اجتماعی برخط حاصل از انتشار اطلاعات با حذف مجموعه پرتاثیرترین عامل‌ها که بر اساس معیار درجه گره و معیار آنتروپی گره اندازه‌گیری شده است. آزمایش‌های این مقاله نشان می‌دهد که الگوریتم پیشنهادی نسبت به روش‌های قبلی، توانایی بیشتری در شناسایی مجموعه گره‌های پرنفوذ دارد، به‌طوری‌که مجموعه باقیمانده گره‌ها از همگنی قابل تنظیمی در معیار نفوذ برخوردار می‌شوند و همچنین معیاری را جهت مشخص نمودن تعداد گره‌های شاخص ارائه می‌کند. حسین نژاد و حاجی کاظم[2] (۲۰۱۸)، در تحقیقی به ارائه مدل اعتماد مبتنی بر شبکه‌های بیزی در شبکه‌های اجتماعی، پرداختند شبکه‌های اجتماعی، شبکه‌هایی هستند که در محیط اینترنت به وجود آمده‌اند و هدف از تاسیس این‌گونه شبکه‌ها کمک به برقراری ارتباط میان افراد مختلف از جوامع گوناگون است، شبکه‌های اجتماعی به شکلی توسعه یافته‌اند که تمام اطلاعات موجود در آن مورد اعتماد هر فردی نیست، شبکه‌ای محبوب است که توان ارائه اطلاعات مورد اعتماد هر شخص را به او ارائه نماید. اگر شخص یا کاربر اطلاعاتی را از دیگران دریافت کند، باید مطمئن باشد که اطلاعات نادرست را از کاربران بدخواه دریافت نکرده است. برای حل این مسائل مدل‌های اعتماد فراوانی توسعه یافته‌اند. با توجه به اینکه اعتماد در واقع با احتمالات سروکار دارد، شبکه بیزین نیز برای حل مسائل از احتمالات استفاده می‌کند، پس شبکه بیزین می‌تواند به کمک محاسبه اعتماد بیاید. این مدل قادر به محاسبه دقیق اعتماد پرداخته و می‌تواند در ابعاد بزرگ‌تر به کمک شبکه‌های اجتماعی بیاید.

راسخی[3] (۲۰۱۶)، با تاکید بر شبکه‌های اجتماعی به بررسی بایسته‌های توسعه امنیت نرم در فضای مجازی پرداخته است که نشان داد یکی از راهکارهای مهم و حائز اهمیت برای امنیت اطلاعات در بستر اینترنت، حیطه‌بندی (جداسازی) شبکه‌ها می‌باشد؛ یعنی از اینترنت و شبکه‌های اطلاع‌رسانی می‌توان با جداسازی شبکه‌ها و بر اساس طبقه‌بندی اطلاعات، استفاده نمود.

حقیقی و غلامعلی[4] (۲۰۱۵)، در تحقیقی عوامل موثر بر اعتمادسازی در شبکه‌های اجتماعی برخط به کمک روش الکتره فازی موردبررسی قرار داده است مسئله شناسایی عوامل تاثیرگذار بر اعتماد از نوع مسائل تصمیم‌گیری چندمعیاره است، ضمن اینکه بیشتر عوامل موثر بر آن با ابهام همراه بوده و قطعی نیستند. به همین دلیل برای دسته‌بندی آن‌ها از روش الکتره فازی بهره برده شده است. با اجرای این روش روی داده‌های جمع‌آوری‌شده از پرسشنامه، مشخص شد با توجه به انواع شبکه‌های اجتماعی، ویژگی‌های «کاربردپذیری»، «پشتیبانی از فناوری به‌روز»، «یکپارچگی» و «میزان برخورداری از اخلاق» در صدر عوامل اثرگذار بر اعتماد کاربران قرار دارند و به‌طورکلی «ویژگی‌های وبگاه» و «ویژگی‌های فناورانه» در مقایسه با «ویژگی‌های امنیتی»، «ویژگی‌های فردی اجتماعی» و «ویژگی‌های فرهنگی کاربر» از اهمیت بیشتری برخوردارند. نتایج به‌دست‌آمده از تحلیل حساسیت در تغییر وزن معیارها نیز نشان می‌دهد ابهام و عدم قطعیت در ورودی‌های مساله تاثیری بر خروجی روش الکتره فازی نمی‌گذارد. کلانتری[5] (۲۰۱۵)، در تحقیقی نقش امنیت در فضای مجازی و شبکه‌های اجتماعی را موردبررسی قرار داده است. فضاهای مجازی محیط‌های تعاملی تحت شبکه‌ای هستند که امکان ارتباط کاربرانی در گروه‌های سنی مختلف را فراهم می‌کنند. این کاربران با اهداف مختلفی از قبیل آموزش، یادگیری، تجارت، امور خیریه و ... در فضای مجازی حضور پیدا می‌کنند. یکی از این فضاهای مجازی شبکه‌های اجتماعی است که به‌طور گسترده‌ای موردتوجه افراد قرار گرفته است. حضور افراد مختلف در چنین فضایی باعث پدید آمدن مسائل امنیتی در آن می‌شود. چرا که کاربران ممکن است با تهدیدهای امنیتی مختلفی مواجه شوند. لذا در این مقاله بعد از ارائه توضیحاتی در مورد فضای مجازی و شبکه‌های مجازی، تهدیدها و نیازمندی‌های امنیتی محیط‌های مجازی به‌ویژه شبکه‌های اجتماعی موردبحث قرار گرفته است.

---

[1] Ghayuri-saleth et al.
[2] Hosseinnejad and Hajikazem
[3] Rasekhi
[4] Haghighi and Gholamali
[5] Kalantari

۲-۳- مطالعات خارجی

التورجمن و سلما[1] (۲۰۲۱)، پژوهشی در مورد امنیت در شبکه‌های اجتماعی انجام دادند و متاسفانه، روندهای فعلی در شبکه‌های اجتماعی به‌طور غیرمستقیم کاربران را ملزم می‌کند تا برای محافظت از محتوای آنلاین خود خط‌مشی بگذارند. الزامات امنیت و حریم خصوصی شبکه‌های اجتماعی هنوز به خوبی درک نشده و یا به‌طور کامل تعریف نشده است. بااین‌وجود، واضح است که آن‌ها کاملا با الزامات کلاسیک امنیت و حریم خصوصی آشنا خواهند بود زیرا شبکه‌های اجتماعی شامل نگرانی‌های کاربر محور هستند و به کاربران متعدد اجازه می‌دهند تا سیاست‌های امنیتی را روی داده‌های مشترک مشخص کنند؛ بنابراین، ما باید تجربه امنیتی عمیقی از حوزه‌ها و فناوری‌های امنیتی متعدد و همچنین دانش گسترده در مورد شبکه‌های اجتماعی را به این حوزه بیاوریم.

لیائو و همکاران[2] (۲۰۲۰) در تحقیقی مدل ارزیابی وضعیت امنیت شبکه بر اساس مارکف پنهان توسعه‌یافته را موردبررسی قرار داده‌اند. در این مقاله یک سیستم ارزیابی وضعیت امنیت شبکه بر اساس مدل مارکوف پنهان توسعه‌یافته طراحی شده است. در مرحله اول، مدل مخفی استاندارد مارکوف از پنج تا به هفت تاپل گسترش می‌یابد و دو پارامتر بهره‌وری دفاع شبکه و بردار از دست دادن خطر اضافه می‌شود تا مدل بتواند وضعیت امنیت شبکه را به‌طور کامل‌تری توصیف کند. سپس، الگوریتم اولیه ماتریس انتقال حالت تعریف شد، بردارهای مشاهده از همجوشی داده‌های مختلف شناسایی امنیت سیستم استخراج شدند، ماتریس انتقال حالت شبکه ایجاد شد و توسط بردارهای مشاهده اصلاح شد و یک روش حل توزیع احتمال پنهان توالی مبتنی بر مدل مخفی پنهان مارکوف استخراج شد. سرانجام، روشی برای محاسبه بردار از دست دادن ریسک طبق تعریف بین‌المللی طراحی شد و مقدار ریسک شبکه فعلی با توزیع احتمال حالت پنهان محاسبه شد. سپس وضعیت امنیت جهانی ارزیابی شد. این آزمایش نشان داد که این مدل از کاربردهای عملی رضایت دارد و نتیجه ارزیابی دقیق و موثر است.

ساگار و واگمار[3] (۲۰۱۶) در تحقیقی اندازه‌گیری امنیت و قابلیت اطمینان از تعیین هویت سایت‌های شبکه‌های اجتماعی را موردبررسی قرار داده‌اند. در این مقاله طرح پیشنهادی جدیدی معرفی شد که در مورد چگونگی انتخاب اعضا برای به حداقل رساندن هجوم‌ها و افزایش امنیت سیستم است. روش‌های مختلف تعیین هویت معرفی شدند که این روش‌های مزایا و معایب خاص خود را دارند. روش پیشنهادی تعیین هویت بر مبنای امنا، برای بازیابی اکانت کاربر استفاده می‌شود که این کار را با ارسال کد امنیتی به امنای کاربر انجام می‌دهد، از سیستم موجود قابل‌اطمینان‌تر است، سیستم موجود از سؤالات امنیتی برای بازیابی اکانت کاربر استفاده می‌کند. استراتژی پیشنهادی از مجموع سه کد تایید برای بازیابی رمز عبور استفاده می‌کند، اما سیستم موجود تنها از یک کد تایید استفاده می‌کند. سیستم پیشنهادی از الگوریتم بلوفیش برای انتشار داده‌ها از یک کاربر به کاربر دیگر استفاده می‌کند و سطح امنیت بالایی را ایجاد می‌کند. الگوریتم بلوفیش برای رمزگذاری و رمزگشایی به کار برده می‌شود. در آینده، این مقاله هجوم‌هایی را در شبکه‌های اجتماعی بررسی خواهد کرد که بر مبنای *SQL* هستند و همچنین سطح قابلیت استفاده از طول چند بیتی را بررسی می‌کند.

عجمی و همکاران[4] (۲۰۱۲) در تحقیقی موضوعات و مسائل حریم خصوصی در شبکه‌های اجتماعی همراه را موردبررسی قرار داده‌اند. این پژوهش نگرانی‌های در ارتباط با مساله حریم خصوصی را با در نظر گرفتن دیدگاه کاربران و پذیرش چنین نرم‌افزارهایی با مشخص کردن انواع متداول آن‌ها ریشه‌یابی نموده که برخی از مکانیزم‌های پیشنهادی برای تایید اطمینان کاربران در تعاملات اجتماعی را مشخص می‌کند.

بر اساس مرور پیشینه پژوهش، مشاهده می‌گردد که تاکنون مطالعه‌ای به شناسایی و رتبه‌بندی شاخص‌های امنیتی شبکه‌های اجتماعی برخط با استفاده از روش تاپسیس در ایران و بالاخص بانک ملی ایران صورت نپذیرفته است؛ بنابراین پژوهش حاضر در صدد پر کردن این شکاف آموزشی و مشارکت در ادبیات پژوهش در این حوزه می‌باشد.

[1] Al-Turjman and Salama
[2] Liao et al.
[3] Sagar and Waghmare
[4] Ajami et al.

امینی و فتحی/ مدیریت نوآوری و راهبردهای عملیاتی، دوره ۳، شماره ۳، پاییز ۱۴۰۱، صفحه: ۳۷۰-۳۵۶

۴- روش پژوهش

در پژوهش حاضر با توجه به موضوع، هدف و اطلاعات مربوط به آن از روش تحقیق توصیفی و پیمایشی استفاده شده است و ازآن‌جایی‌که این تحقیق در یک سازمان واقعی، عینی و زنده (پویا) صورت گرفته است و از نتایج آن می‌توان به‌طور عملی استفاده کرد، یک تحقیق کاربردی می‌باشد.

با توجه به هدف پژوهش که همانا شناسایی و رتبه‌بندی شاخص‌های امنیتی در شبکه‌های اجتماعی بر خط می‌باشد، مراحل زیر جهت انجام پژوهش صورت گرفت (**شکل ١**).



شکل ١- فرآیند انجام پژوهش.

Figure 1- Research process.

در پایان نیز برای اولویت‌بندی شاخص‌ها از تکنیک *TOPSIS* استفاده می‌گردد و درنهایت با استفاده از آزمون همبستگی اسپیرمن به بررسی ارتباط بین شاخص‌های شناسایی شده و امنیت در شبکه‌های اجتماعی بر خط پرداخته شده است. بدین منظور نیز پرسشنامه‌ای با ٢٤ گویه توزیع شد.

٤-١- جامعه و نمونه آماری

جامعه آماری این مطالعه را کلیه پرسنل واحدهای فناوری اطلاعات بانک ملی که حدود ٩٠٠ نفر هستند می باشد که با فرمول کوکران ٢٦٢ نفر به‌عنوان نمونه آماری انتخاب شد. برای سنجش پایایی پرسشنامه مقیاس زوجی از نرخ ناسازگاری استفاده شده است و روایی آن توسط متخصصین تایید شده است.

٤-٢- تکنیک تاپسیس

این روش توسط هوانگ و یون[1] (١٩٨١) ارائه گردید. در این روش *m* عامل یا گزینه به وسیله یك فرد یا گروهی از افراد تصمیم‌گیرنده مورد ارزیابی قرار می‌گیرند. این تکنیك بر این مفهوم بنا شده است که هر عامل انتخابی باید کمترین فاصله را با عامل ایده‌آل مثبت (مهم‌ترین)

[1] Hwang and Yoon

و بیشترین فاصله را با عامل ایده‌آل منفی (کم‌اهمیت‌ترین عامل) داشته باشد به‌عبارت‌دیگر در این روش میزان فاصله یك عامل با عامل ایده‌آل مثبت و منفی سنجیده شده و این خود معیار درجه‌بندی و اولویت‌بندی عوامل است (آذر و رجب زاده[1]، ۲۰۱۷). مراحل این روش عبارت‌اند از:

۱. تعیین ماتریس مقایسه عوامل: در این مرحله ماتریسی رسم خواهد شد که در سطر آن عوامل و در ستون آن افراد نظر دهنده آورده می‌شود و در تلاقی سطر و ستون، میزان اهمیتی که هر پاسخگو برای هر کدام از عوامل قائل شده است، آورده می‌شود.

R_{ij}: نظر فرد ith درباره عامل jth که در مقیاس ۷ گزینه‌ای طیف لیکرت (۱ تا ۷) بیان شده است.

۲. بهنجار کردن ماتریس تصمیم‌گیری: به‌منظور قابل‌مقایسه شدن، مقیاس‌های مختلف اندازه‌گیری ماتریس تصمیم‌گیری به ماتریس بهنجار شده یا ماتریس بی‌مقیاس موزون با استفاده از **رابطه (۱)** تبدیل می‌شوند.

$$n_{ij} = \frac{r_{ij}}{\sqrt{\sum_{i=1}^{m} {r_{ij}}^2}} \qquad (۱)$$

۳. تعیین عامل ایده‌آل مثبت و ایده‌آل منفی: در این مرحله بایستی عوامل که از نظر پاسخ‌دهندگان به‌عنوان مهم‌ترین عامل و کم‌اهمیت‌ترین عوامل مشخص شده‌اند، شناسایی شوند **رابطه (۲)**:

$$\text{گزینه ایده‌آل مثبت} = A^{+} = \left\{ \left(\max_{i} V_{ij} \mid j \in J \right), i = 1,2,\ldots,m \right\} = \left\{ V_1^{+}, V_2^{+}, \ldots, V_n^{+} \right\}$$

$$\text{گزینه ایده‌آل منفی} = A^{-} = \left\{ \left(\min_{i} V_{ij} \mid j \in J \right), i = 1,2,\ldots,m \right\} = \left\{ V_1^{-}, V_2^{-}, \ldots, V_n^{-} \right\} \qquad (۲)$$

٤. محاسبه اندازه جدایی (فاصله): در این مرحله بایستی میزان فاصله هریک از عوامل از ایده‌آل مثبت و ایده‌آل منفی تعیین شود؛ بنابراین فاصله گزینه ith با ایده‌آل‌ها با استفاده از روش اقلیدسی به شرح **رابطه (۳)** است:

$$\text{فاصله گزینه ith از ایده‌آل مثبت} = d_i^{+} = \left\{ \sum_{j=1}^{n} \left(V_{ij} - V_j^{+} \right)^2 \right\}^{0/5} ; i = 1,2,\ldots,m$$

$$\text{فاصله گزینه ith از ایده‌آل منفی} = d_i^{-} = \left\{ \sum_{j=1}^{n} \left(V_{ij} - V_j^{-} \right)^2 \right\}^{0/5} ; i = 1,2,\ldots,m \qquad (۳)$$

۵. محاسبه میزان نزدیکی هر کدام از عوامل به عامل ایده‌آل مثبت و ایده‌آل منفی: محاسبه مقدار C_i بر اساس **رابطه (٤)**:

$$c_i = \frac{\text{مقدار فاصله با ایده آل منفی}}{\text{مقدار فاصله با ایده آل منفی}} \qquad (۴)$$

و دسته‌بندی عوامل بر اساس ترتیبی نزولی C_i. به‌عبارت‌دیگر C_i هرچه بالاتر باشد درجه اهمیت عامل بالاتر است.

۵- یافته‌های پژوهش

۱-۵- اطلاعات جمعیت شناختی

تحلیل توصیفی داده‌های مربوط به مشخصات پاسخ‌دهندگان در **جدول ۱** آورده شده است.

---

[1] Azar and Rajabzadeh

جدول ۱- اطلاعات جمعیت شناختی پاسخ‌دهندگان.

Table 1- Demographic information of the respondents.

متغیر		فراوانی (نفر)	درصد فراوانی
سن	زیر ۳۰ سال	74	28.2%
	۳۱ تا ۴۰	95	36.3%
	۴۱ تا ۵۰	52	19.8%
	بالای ۵۰ سال	41	15.6%
جنسیت	مرد	217	82.8%
	زن	45	17.2%
تحصیلات	کاردانی و پایین‌تر	72	27.5%
	کارشناسی	117	44.7%
	کارشناسی ارشد	59	22.5%
	دکتری	14	5.3%
سابقه کار	کمتر از ۵ سال	108	41.2%
	بین ۶ تا ۱۰ سال	96	36.6%
	بین ۱۱ تا ۲۰ سال	41	15.6%
	بیشتر از ۲۰ سال	17	6.4%

۲-۵- آزمون توزیع داده‌ها

برای بررسی نرمال بودن متغیرها از آزمون کلموگروف – اسمیرنوف استفاده شده است. در این آزمون فرضیه‌ی صفر نرمال بودن داده‌ها است، اگر میزان *K-S* بین ۱/۹۶+ و ۱/۹۶- باشد و سطح معنی‌داری بیشتر از ۰/۰۵ باشد، فرضیه صفر رد می‌شود و نرمال بودن داده‌ها تایید می‌شود. **جدول ۲** نتایج آزمون کلموگروف – اسمیرنوف را نشان می‌دهد که حاکی از توزیع غیرنرمال داده‌ها می‌باشد.

جدول ۲- نتایج آزمون نرمال بودن توزیع داده‌ها.

Table 2- The results of the normality test of data distribution.

متغیرها	میانگین	میزان K-S	سطح معناداری	نتیجه
۱) پیاده‌سازی سازوکارهای تصدیق هویت و مجوزدهی	3.1	1.9	0	غیر نرمال
۲) استفاده از نرم‌افزارهای به‌روز و پرهیز از نرم‌افزارها و برنامه‌های مشکوک	2.9	2.3	0	غیر نرمال
۳) محدودیت انتشار اطلاعات شخصی	3.3	1.4	0	غیر نرمال
۴) بین پایش به‌منظور عدم‌پردازش غیرمجاز اطلاعات	3	1.8	0	غیر نرمال
۵) رعایت استانداردهای امنیتی	3	2.4	0	غیر نرمال
۶) زیرساخت‌های IT کشور	2.9	1.9	0	غیر نرمال
۷) نصب سیستم شناساگر متجاوز	3.1	1.5	0	غیر نرمال

در این پژوهش، تمامی شاخص‌های تحقیق دارای سطح معناداری کمتر از ۰/۰۵ هستند که توزیع غیر نرمال داده‌ها را تایید می‌کند؛ بنابراین، برای انجام آزمون فرضیه‌های تحقیق باید از آزمون‌های ناپارامتریک استفاده شود که در ادامه به‌منظور آزمون همبستگی متغیرها از آزمون ناپارامتریک همبستگی اسپیرمن استفاده شده است.

۳-۵- آزمون همبستگی اسپیرمن

در این بخش آزمون فرضیه‌های تحقیق ارائه شده است. متغیر وابسته پژوهش «امنیت در شبکه‌های اجتماعی بر خط» می‌باشد و متغیرهای مستقل، شاخص‌های شناسایی‌شده (هفت مورد) می‌باشند که در **جدول ۳** نتایج آزمون همبستگی اسپیرمن ارائه شده است.

امینی و فتحی/ مدیریت نوآوری و راهبردهای عملیاتی، دوره ۳، شماره ۳، پاییز ۱۴۰۱، صفحه: ۲۷۰-۲۵۶

جدول ۳- نتایج آزمون همبستگی اسپیرمن.
Table 3- Spearman's correlation test results.

فرضیه	رابطه	ضریب همبستگی	میزان معناداری	N	نتیجه
1	پیاده‌سازی سازوکارهای تصدیق هویت و مجوزدهی ← امنیت شبکه‌های اجتماعی بر خط	0.324	0	262	تایید
2	استفاده از نرم‌افزارهای به‌روز و پرهیز از نرم‌افزارها و برنامه‌های مشکوک← امنیت شبکه‌های اجتماعی بر خط	0.230	0	262	تایید
3	محدودیت انتشار اطلاعات شخصی← امنیت شبکه‌های اجتماعی بر خط	0.244	0.04	262	تایید
4	پایش به‌منظور عدم‌پردازش غیرمجاز اطلاعات← امنیت شبکه‌های اجتماعی بر خط	0.271	0	262	تایید
5	رعایت استانداردهای امنیتی ← امنیت شبکه‌های اجتماعی بر خط	0.174	0	262	تایید
6	زیرساخت‌های IT کشور← امنیت شبکه‌های اجتماعی بر خط	0.283	0	262	تایید
7	نصب سیستم شناساگر متجاوزر← امنیت شبکه‌های اجتماعی بر خط	0.214	0	262	تایید

۵-۵- رتبه‌بندی معیارها با روش تاپسیس

در این تحقیق برای رتبه‌بندی شاخص‌های امنیتی در شبکه‌های اجتماعی بر خط از تکنیک *TOPSIS* استفاده شده است. ماتریس تصمیم‌گیری و اوزان معیارهای موثر امنیتی در شبکه‌های اجتماعی بر خط که پیش‌تر از طریق نتایج پرسشنامه مقایسات زوجی از نظرات خبرگان محاسبه گردیده بود بدین ترتیب به دست آمد که در **جدول ٤** قابل مشاهده است.

جدول ۴- ماتریس تصمیم اولیه.
Table 4- Primary decision matrix.

	معیار ۱	معیار ۲	معیار ۳	معیار ۴	معیار ۵	معیار ۶	معیار ۷
معیار ۱	1	0.1969	0.1969	0.1969	0.1969	0.1969	0.1969
معیار ۲	0.1472	1	0.1472	0.1472	0.1472	0.1472	0.1472
معیار ۳	0.1091	0.1091	1	0.1091	0.1091	0.1091	0.1091
معیار ۴	0.1274	0.1274	0.1274	1	0.1274	0.1274	0.1274
معیار ۵	0.1393	0.1393	0.1393	0.1393	1	0.1393	0.1393
معیار ۶	0.151	0.151	0.151	0.151	0.151	1	0.151
معیار ۷	0.1292	0.1292	0.1292	0.1292	0.1292	0.1292	1

در ادامه، ماتریس تصمیم نرمالیزه‌شده نیز در **جدول ۵** مشاهده می‌شود.

جدول ۵- ماتریس تصمیم بی‌مقیاس شده (نرمال شده).
Table 5- Unscaled (normalized) decision matrix.

	معیار ۱	معیار ۲	معیار ۳	معیار ۴	معیار ۵	معیار ۶	معیار ۷
معیار ۱	0.9497	0.1855	0.1847	0.1851	0.1854	0.1856	0.1851
معیار ۲	0.1398	0.9425	0.1382	0.1384	0.1386	0.1388	0.1384
معیار ۳	0.1036	0.1028	0.9384	0.1026	0.1027	0.1029	0.1026
معیار ۴	0.121	0.1201	0.1195	0.9402	0.1199	0.1201	0.1198
معیار ۵	0.1323	0.1313	0.1307	0.1309	0.9415	0.1313	0.131
معیار ۶	0.1434	0.1423	0.1417	0.142	0.1422	0.943	0.142
معیار ۷	0.1227	0.1218	0.1212	0.1215	0.1216	0.1218	0.9404

در گام بعدی، ماتریس نرمالیزه‌شده وزنی محاسبه شده است که در **جدول ٦** مشاهده می‌شود.

جدول ۶- ماتریس تصمیم نرمال شده موزون.

Table 6- Weighted normalized decision matrix.

	معیار ۱	معیار ۲	معیار ۳	معیار ۴	معیار ۵	معیار ۶	معیار ۷
معیار ۱	0.187	0.0273	0.0202	0.0236	0.0258	0.028	0.0239
معیار ۲	0.0275	0.1388	0.0151	0.0176	0.0193	0.021	0.0179
معیار ۳	0.0204	0.0151	0.1024	0.0131	0.0143	0.0155	0.0133
معیار ۴	0.0238	0.0177	0.013	0.1198	0.0167	0.0181	0.0155
معیار ۵	0.026	0.0193	0.0143	0.0167	0.1311	0.0198	0.0169
معیار ۶	0.0282	0.0209	0.0155	0.0181	0.0198	0.1424	0.0183
معیار ۷	0.0242	0.0179	0.0132	0.0155	0.0169	0.0184	0.1215

در مرحله بعد، مجموعه نقاط ایده‌آل مثبت و منفی با به دست خواهند آمد. نقاط ایده‌آل مثبت، فاصله از ایده‌آل مثبت و نقاط ایده‌آل منفی، فاصله از ایده‌آل منفی را نشان می‌دهند. **جدول ۷** و **جدول ۸** مجموعه نقاط ایده‌آل مثبت و منفی را نشان می‌دهند.

جدول ۷- مجموعه نقاط ایده‌آل مثبت.

Table 7- Set of positive ideal points.

	معیار ۱	معیار ۲	معیار ۳	معیار ۴	معیار ۵	معیار ۶	معیار ۷	مجموع مربعات هر سطر	فاصله از ایده‌آل مثبت (Si+)
معیار ۱	0.187	0.0273	0.0202	0.0236	0.0258	0.028	0.0239	0.0621	0.2492
معیار ۲	0.0275	0.1388	0.0151	0.0176	0.0193	0.021	0.0179	0.0815	0.2854
معیار ۳	0.0204	0.0151	0.1024	0.0131	0.0143	0.0155	0.0133	0.0959	0.3096
معیار ۴	0.0238	0.0177	0.013	0.1198	0.0167	0.0181	0.0155	0.089	0.2984
معیار ۵	0.026	0.0193	0.0143	0.0167	0.1311	0.0198	0.0169	0.0845	0.2907
معیار ۶	0.0282	0.0209	0.0155	0.0181	0.0198	0.1424	0.0183	0.08	0.2828
معیار ۷	0.0242	0.0179	0.0132	0.0155	0.0169	0.0184	0.1215	0.0883	0.2972

جدول ۸- مجموعه نقاط ایده‌آل منفی.

Table 8- Set of negative ideal points.

	معیار ۱	معیار ۲	معیار ۳	معیار ۴	معیار ۵	معیار ۶	معیار ۷	مجموع مربعات هر سطر	فاصله از ایده ال منفی (Si^-)
معیار ۱	0.1666	0.0122	0.0071	0.0105	0.0115	0.0125	0.0107	0.0285	0.1687
معیار ۲	0.0071	0.1236	0.002	0.0046	0.005	0.0054	0.0046	0.0154	0.1242
معیار ۳	0	0	0.0893	0	0	0	0	0.008	0.0893
معیار ۴	0.0034	0.0025	0	0.1067	0.0024	0.0026	0.0022	0.0114	0.1069
معیار ۵	0.0056	0.0042	0.0012	0.0036	0.1168	0.0043	0.0037	0.0137	0.1172
معیار ۶	0.0078	0.0058	0.0024	0.005	0.0055	0.1268	0.0051	0.0163	0.1276
معیار ۷	0.0038	0.0028	0.0002	0.0024	0.0026	0.0029	0.1082	0.0118	0.1084

همان‌طور که مشاهده می‌گردد در دو ستون آخر **جدول ۷** و **جدول ۸** فاصله هر گزینه از حل ایده‌آل مثبت و منفی برای هر معیار با جذر گرفتن از مجموع مربعات هر سطر نیز محاسبه شده است. هر چه فاصله شاخص‌ها از ایده‌آل مثبت (Si^+) کمتر و از ایده‌آل منفی (Si^-) بیشتر باشد، از اولویت بالاتری برخوردار خواهند بود. ضریب نزدیکی (Ci) نیز بیانگر درجه اهمیت شاخص‌هاست. بدین معنا که هرچه ضریب نزدیکی بیشتر باشد، متغیرها از رتبه بهتری برخوردار خواهند بود. مجموعه فواصل از نقاط ایده‌آل مثبت، منفی، ضریب نزدیکی و رتبه نهایی متغیرها در **جدول ۹** آورده شده است.

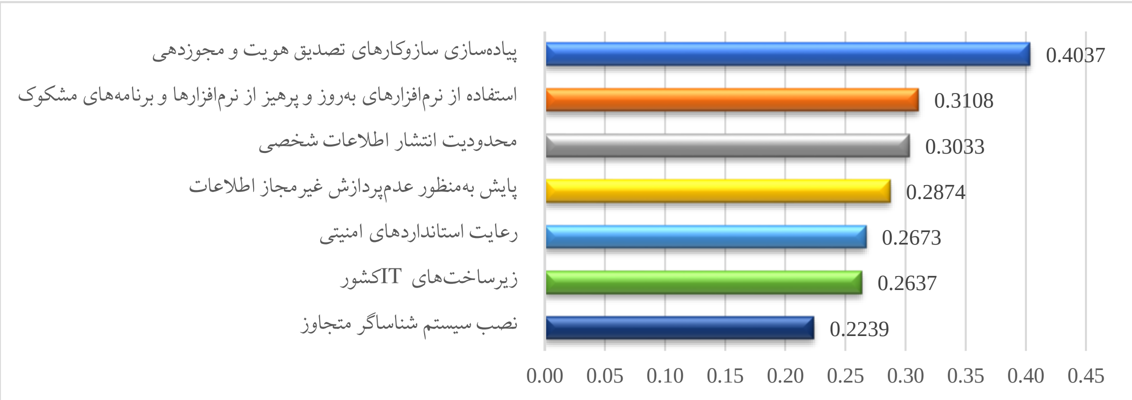
جدول ۹- فواصل از نقاط ایده‌آل مثبت، منفی و ضریب نزدیکی معیارها.
Table 9- Distances from positive and negative ideal points and the proximity coefficient of criteria.

عوامل	اندازه فاصله به‌ازای راه‌حل ایده‌آل مثبت (Si^+)	اندازه فاصله به‌ازای راه‌حل ایده‌آل منفی (Si^-)	ضریب نزدیکی C^*
معیار ۱	0.2492	0.1687	0.4037
معیار ۲	0.2854	0.1242	0.3033
معیار ۳	0.3096	0.0893	0.2239
معیار ۴	0.2984	0.1069	0.2637
معیار ۵	0.2907	0.1172	0.2874
معیار ۶	0.2828	0.1276	0.3108
معیار ۷	0.2972	0.1084	0.2673

بنابراین، همان‌گونه که در **جدول ۱۰** و **شکل ۱** مشاهده می‌گردد، رتبه‌بندی نهایی معیارهای امنیتی در شبکه‌های اجتماعی بر خط با استفاده از روش تاپسیس انجام پذیرفته است که به ترتیب اهمیت لیست شده‌اند.

جدول ۱۰- رتبه‌بندی معیارها با استفاده از روش تاپسیس.
Table 10- Rating of criteria using TOPSIS method.

عوامل	C^*	رتبه
معیار ۱: پیاده‌سازی سازوکارهای تصدیق هویت و مجوزدهی	0.4037	1
معیار ۶: استفاده از نرم‌افزارهای به‌روز و پرهیز از نرم‌افزارها و برنامه‌های مشکوک	0.3108	2
معیار ۲: محدودیت انتشار اطلاعات شخصی	0.3033	3
معیار ۵: پایش به‌منظور عدم‌پردازش غیرمجاز اطلاعات	0.2874	4
معیار ۷: رعایت استانداردهای امنیتی	0.2673	5
معیار ۴: زیرساخت‌های IT کشور	0.2637	6
معیار ۳: نصب سیستم شناساگر متجاوز	0.2239	7



شکل ۱- رتبه‌بندی معیارهای امنیتی در شبکه‌های اجتماعی بر خط.
Figure 1- Ranking of security criteria in online social networks.

۶- بحث و نتیجه‌گیری

عامل امنیت به عنوان پایه اساسی روابط و تعاملات افراد در کانون توجه قرار گرفته است؛ به‌ویژه هنگامی‌که ضرر و منفعت مالی در میان باشد. ازاین‌رو اغلب مطالعات پیشین در زمینه اعتماد در بستر اینترنت و محیط الکترونیکی، اعتماد را با رویکرد تجاری بررسی کرده‌اند. اگرچه در شبکه‌های اجتماعی الکترونیکی موضوع پول و ریسک مالی مطرح نیست، با تاملی عمیق می‌توان دریافت اطلاعات به اشتراک گذاشته شده کاربران که در بعضی مواقع شخصی است، ارزش و ریسک کمتری از جنبه مالی ندارد؛ به‌ویژه سوءاستفاده و استفاده هدفمند از این اطلاعات رو به افزایش است و بسیاری از شبکه‌ها بر مبنای کسب درآمد با استفاده از شناخت افراد از طریق اطلاعات به اشتراک گذاشته شده پایه‌ریزی شده‌اند. اغلب مطالعاتی که به موضوع اعتماد در شبکه‌های اجتماعی پرداخته‌اند، به دلیل ماهیت این‌گونه وبگاه‌ها، بیشتر از نظر ساختاری یا رتبه‌دهی هر یک از کاربران به محتوای کاربر دیگر، اعتماد کاربران این وبگاه‌ها را سنجیده‌اند. ازاین‌رو مقاله حاضر

ضمن شناسایی معیارهای امنیتی در شبکه‌های اجتماعی بر خط، با بهره‌مندی از مطالعات پیشین در این زمینه و ارائه مدلی، به رتبه‌بندی این عوامل اقدام کرده است.

ما در این تحقیق به این نتیجه رسیدیم که بین عوامل موثر و امنیت شبکه‌های اجتماعی بر خط تعریف‌شده برای این شبکه‌ها، رابطه معناداری دارد. در واقع توسعه‌ی زیرساخت‌های فناوری اطلاعات و ارتباطات و افزایش شمار کاربران استفاده‌کننده از شبکه‌های اجتماعی مجازی، لزوم ایجاد و توسعه‌ی سازوکاری برای برقراری امنیت در این شبکه‌های ارتباطی را توجیه می‌کند. از سوی دیگر، رشد فزاینده‌ی جرایم در حوزه فضای تولید و تبادل اطلاعات مجازی مانند، جعل داده‌ها و عناوین، سرقت اطلاعات، تجاوز به حریم خصوصی اشخاص و گروه‌ها ایجاب می‌کند که یک منبع تخصصی و قانونی و رسمی وجود داشته باشد که توان پیگیری و رسیدگی به این‌گونه از جرایم را داشته باشد. وجود چنین منابعی همان‌گونه که نتایج این تحقیق نشان داد موجب بالا رفتن امنیت در این فضا و محتوای آن‌ها می‌گردد. ولی شاید بتوان اظهار داشت که به دلیل آگاهی پایین کاربران از وجود و حدود وظایف منابع ضمانت اجرایی در شبکه‌های اجتماعی مجازی، شدت رابطه‌ی بین این ضامن‌های قانونی و امنیت شبکه‌های اجتماعی مجازی و محتوای آن‌ها ضعیف می‌باشد. نتایج به دست آمده با نتایج تحقیقات (ساگار و واگمار، ۲۰۱۶؛ لیائو و همکاران، ۲۰۲۰؛ عجمی و همکاران، ۲۰۱۲) همسو می‌باشد.

این مطالعه هم مانند مطالعاتی که در حوزه علوم اجتماعی صورت می‌گیرد به دلیل ارتباط نزدیک با افراد موردمطالعه و سیالت موضوع و افراد به دلیل تنوع گسترده با مشکلات عدیده‌ای روبه‌رو بوده که یکی از آن محدودیت‌ها این امر بوده که کارهای پژوهشی که عوامل دخیل در امنیت شبکه‌های اجتماعی را به‌صورت تخصصی سنجش کرده باشد بسیار محدود و کم بوده است.

با توجه به اینکه پژوهش حاضر درصدد بررسی یک موضوع حیاتی در حوزه امنیت شبکه‌های اجتماعی مجازی بوده است و بنا بر روشی که در پژوهش به کار رفته شد تا ابعاد نظری و دلالت‌های اجتماعی به‌صورت تجربی سنجش شود و همچنین نتایجی که در این مطالعه به دست آمد شایسته است این پژوهش در ابعاد گسترده‌تری نیز موردبررسی قرار گیرد. همچنین با توجه به گستردگی و استفاده‌ی جمعیت بالایی جامعه از شبکه‌های اجتماعی مجازی، پیشنهاد می‌گردد تحقیقاتی این‌چنینی از دیدگاه نقش‌های دیگر در جامعه نیز صورت بگیرد و دور از انتظار نیست که نتایج متنوعی به دست آید.

منابع

Azar, A., & Rajabzadeh, A. (2017). *Applied decision making (MADM approach)*. Negahe Danesh. (**In Persian**). https://www.gisoom.com

Ahmadi, A., & Vaezi, A. (2019). An approach to increase security and privacy on social media *.4th international conference on applied research in science and engineering*, Tehran, Iran. Civilcia. (**In Persian**). https://civilica.com/doc/1000645/

Babaei, B (2018). Threats of cyberspace and social networks in NAJA internal security. *Journal of law enforcement and security studies*, *13*(47), 129-154. (**In Persian**). https://www.magiran.com/paper/1970526

Rasooli, M. R, & Bandegi Monfared, S. (2014). Content analysis of cultural and social themes in social networks (case study: Facebook and the youth of Tehran), *Culture studies - communication*, *15*(27), 67-85. (**In Persian**). https://www.sid.ir/paper/395229/fa

Haghighi, E., & Gholamali, M. (2015). Identifying the factors affecting trust building in online social networks using fuzzy ELECTRE method. *Information technology management, 7*(4), 715-740. (**In Persian**). DOI: 10.22059/jitm.2015.54750

Hosseinnejad, V., & Hajikazem, A. A. (2018). Bayesian network-based trust model in social networks, *Journal of electronic defense and cyber defense*, *6*(2), 29-38. (**In Persian**). https://www.magiran.com/paper/1902588

Rasekhi, A. (2016). Requirements for the development of soft security in cyberspace with emphasis on social networks. *Police protection and security studies quarterly*, *11*(38), 1-39. (**In Persian**). http://spaps.jrl.police.ir/article_13760.html?lang=en

Rasouli, Y. S., & Jafari, M. (2020). Investigating and comparing how cryptographic algorithms work in network security. *The 4th international conference on new strategies in engineering, information science and technology in the next century.* Alborz, Iran. Civilcia. (**In Persian**). https://civilica.com/doc/1032523

Zare, M. H., Norouzi, E. (2019). Assessing the security of social networks of the particle cluster algorithm. *Conference on computer science, electrical and telecommunication Engineering*, Mashhad, Iran. Civilcia. (**In Persian**). https://civilica.com/doc/988314/

Zarezadeh, r. (2021). disadvantages and security challenges of internal issues; a case study of virtual social networks. *Journal of strategic studies, 2(92), 7-32.* (**In Persian**). http://ensani.ir

Doaguyan, D., & Kheirandish, M. R. (2021). The effect of mobile social networks under the social relations of families in the western regions of greater Tehran (telegram case study). *Journal of security and law enforcement studies*, *14*(53), 131-156. (**In Persian**). http://spaps.jrl.police.ir/article_93867.html?lang=en

Sahafizadeh, E., & Torkladani, B. (2020). Control of rumors on social networks using soft security mechanisms. *The 17th international conference of the iranian password association*, Tehran, Iran. Civilcia. (**In Persian**). https://civilica.com/doc/1120274

Abdulrahmani, R., Mozafari, M. M., & Mohamadi, I. (2018). Analyzing the security content of Telegram social network messages. *Strategy*, *27*(89), 125-150. (**In Persian**). https://www.sid.ir/paper/405216/fa

Ghayuri-saleth, M., Bazdar, Gh. R., & Sarkardei, A. (2018). Influential factors in disseminating information on social networks based on entropy theory. *Electronic and cyber defense*, *2*(22), 1-10. (**In Persian**). https://www.sid.ir/paper/243160/fa

Kalantari, S. (2015). The role of security in cyberspace and social networks. *The first national conference on computer, information technology and Islamic communications in Iran,* Qom, Iran. Civilcia. (**In Persian**). https://civilica.com/doc/408879

Mohamadrezae, M. R. (2021). Detection of fake users in social networks using principal component analysis and kernel density estimation algorithm (case study: on twitter social network). *Electronic and cyber defense*, *9*(3), 109-123. (**In Persian**). https://ecdj.ihu.ac.ir/article_205996.html

Mohkamkar, I., & Halaj, M. M. (2014). Cyberspace, its dimensions, features and functions in the field of identity with the focus on virtual social networks. *Journal of knowledge*, *23* (201), 63-82. (**In Persian**). http://ensani.ir/file/download/article/20150617145855-9723-377.pdf

Mohamadi, Z., Delsooz, K., & Sayah, E. (2019). Filtering social networks and its role in protecting and securing civil rights in cyber defense in Iran. *The 2nd national conference on cyber defense,* Maraqeh, Iran. Civilcia. (**In Persian**). https://civilica.com/doc/903767/

Mehregan, A., & Sedqivash, M. (2020). Study and review of security solutions in social networks. *The 4th national conference on computer science and technology of Iran*, Tehran, Iran. Civilcia. (**In Persian**). https://civilica.com/doc/1116856/

Nadri, Gh. R., Bakhshayeshhi, A., Darabi, A., & Maghsudi, M. (2019).). Investigating the political-security role of virtual social networks on national security of Iran. *Protection and security research*, *8*(29), 63-88. (**In Persian**).https://www.sid.ir/paper/265958/fa

Blumenstock, J. E., Chi, G., & Tan, X. (2019). *Migration and the value of social networks*. Retrived from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3360078#

Chaffey, D. (2022). *Global social media research summary 2018.* Retrieved from https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research

Edosomwan, S., Prakasan, S. K., Kouame, D., Watson, J., & Seymour, T. (2011). The history of social media and its impact on business. *Journal of applied management and entrepreneurship*, *16*(3), 79-91. https://www.proquest.com/openview/f828806820e0b99fcbda9c765788e137/1?pq-origsite=gscholar&cbl=25565

Al-Turjman, F., & Salama, R. (2021). Security in social networks. In *Security in IoT social networks* (pp. 1-27). Academic Press. DOI: https://doi.org/10.1016/B978-0-12-821599-9.00001-7

Hwang, C. L., & Yoon, K. (1981). Methods for multiple attribute decision making. In *Multiple attribute decision making* (pp. 58-191). Springer, Berlin, Heidelberg. 58-191. DOI: https://doi.org/10.1007/978-3-642-48318-9_3

Sagar, K., & Waghmare, V. (2016). Measuring the security and reliability of authentication of social networking sites. *Procedia computer science*, *79*, 668-674. DOI: https://doi.org/10.1016/j.procs.2016.03.085

McCarroll, N., & Curran, K. (2013). Social networking in education. *International journal of innovation in the digital economy (IJIDE)*, *4*(1), 1-15. DOI:10.4018/978-1-4666-6114-1.ch034

Ortiz-Ospina, E. (2019). *The rise of social media*. Our world in data. https://ourworldindata.org/rise-of-social-media

Ajami, R., Al Qirim, N., & Ramadan, N. (2012). Privacy issues in mobile social networks. *Procedia computer science*, *10*, 672-679. DOI: https://doi.org/10.1016/j.procs.2012.06.086

Liao, Y., Zhao, G., Wang, J., & Li, S. (2020). Network security situation assessment model based on extended hidden Markov. *Mathematical problems in engineering*, *2020*. DOI: https://doi.org/10.1155/2020/1428056

Zeebaree, S., Ameen, S., & Sadeeq, M. (2020). Social media networks security threats, risks and recommendation: A case study in the kurdistan region. *International journal of innovation, creativity and change*, *13*(7), 349-365.

امینی و فتحی/ مدیریت نوآوری و راهبردهای عملیاتی، دوره ۳، شماره ۳، پاییز ۱۴۰۱، صفحه: ۳۵۶-۳۷۰